

Signal Space Alignment for an Encryption Message and Successive Network Code Decoding on the MIMO K -way Relay Channel

Namyoon Lee[†] and Joohwan Chun[‡]

[†]Samsung Advanced Institute of Technology (SAIT), Yongin-si, Korea

[‡]Electrical Engineering department, KAIST, Daejeon, Korea

E-mail: namyoon.lee@gmail.com, and chun@ee.kaist.ac.kr

Abstract—This paper investigates a network information flow problem for a multiple-input multiple-output (MIMO) Gaussian wireless network with K -users and a single intermediate relay having M antennas. In this network, each user intends to convey a multicast message to all other users while receiving $K - 1$ independent messages from the other users via an intermediate relay. This network information flow is termed a MIMO Gaussian K -way relay channel. For this channel, we show that $\frac{K}{2}$ degrees of freedom is achievable if $M = K - 1$. To demonstrate this, we come up with an encoding and decoding strategy inspired from cryptography theory. The proposed encoding and decoding strategy involves a *signal space alignment for an encryption message* for the multiple access phase (MAC) and *zero forcing with successive network code decoding* for the broadcast (BC) phase. The idea of the *signal space alignment for an encryption message* is that all users cooperatively choose the precoding vectors to transmit the message so that the relay can receive a proper encryption message with a special structure, *network code chain structure*. During the BC phase, *zero forcing combined with successive network code decoding* enables all users to decipher the encryption message from the relay despite the fact that they all have different self-information which they use as a key.

I. INTRODUCTION

Two-way communication or bidirectional communication between two nodes was first considered by Shannon [1]. By involving a relay node between two nodes, the two-way relay channel has drawn great interest from numerous researchers due to its useful application scenarios in cellular and ad-hoc networks. Several studies [2]-[9] showed that the sum-rate performance of the two-way relaying protocol significantly increases compared with that of one-way relay protocol.

Recently, the two-way relay channel has been generalized in various network information flow settings. To realize multi-pairs information exchange, the authors in [10]-[12] studied a multi-pair two-way relay channel in which the relay helps the communication between multiple pairs of users. In [10], authors proposed a jointly demodulate-and-XOR forward relaying scheme for a code-division multiple access system under an interference-limited environment. In addition, other authors [11]-[12] characterized the capacity of a multi-pair relay channel in a deterministic channel model. They showed that a divide-and-conquer strategy exploiting signal-level alignment for the MAC phase and a simple equation-forwarding scheme

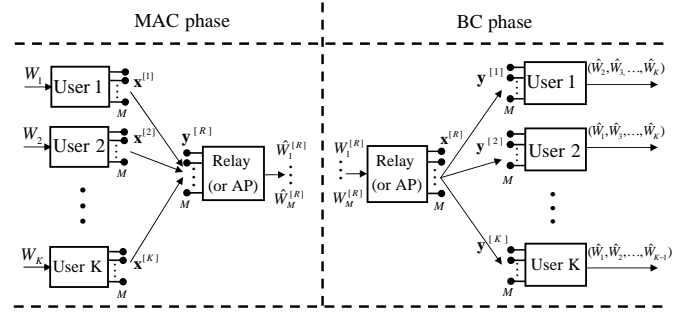


Fig. 1. System model of MIMO Gaussian K -way relay channel.

for the broadcast phase (BC) achieve the capacity for a deterministic channel case. They also showed these schemes extended to a Gaussian channel case for achieving the capacity within a constant number of bits.

Furthermore, the authors in [13]-[15] investigated multiuser and multi-way relay communications, which are more general scenarios than the use of a multi-pair two-way relay channel in the terms of multiple directions of communication. In [13], for several relaying schemes, examined the achievable rate regions of a multi-way relay channel with multiple clusters of users such that the users in each cluster want to exchange multicast message within that group of users. By considering multiple unicast messages per user, in our previous works [14]-[15], an efficient coding scheme termed the *signal space alignment for network coding* was proposed for a multiple-input-multiple-output (MIMO) Gaussian Y channel. Using this scheme in [15], the authors showed that the degrees of freedom for the MIMO Gaussian Y channel is $3M \log(\text{SNR}) + o(\log(\text{SNR}))$ when each user has M antennas and when the relay has $N \geq \lceil \frac{3M}{2} \rceil$ antennas. From this scheme, the authors demonstrated how to deal with multiple interference signals on multi-user and multi-way communications by appropriately exploiting interference alignment [16] and network coding [6]-[9].

In this paper we investigate a network information flow problem for a MIMO Gaussian wireless network with K -users and a single intermediate relay having M antennas i.e., the single cluster multi-way relay channel in one of the previous

studies [13]. In this network, user i , $i = \{1, 2, \dots, K\}$ wants to convey a multicast message W_i to all other users, while receiving $K - 1$ independent messages from the other users via the intermediate relay. This network information flow is termed a MIMO Gaussian K -way relay channel. There are various interesting application scenarios of the MIMO Gaussian K -way relay channel, such as video conferencing using Wi-Fi access point and multi-player gaming using smart phones.

In this paper, we propose an encoding and decoding strategy which were inspired by cryptography theory. In cryptography, encryption is a process of transforming information using an algorithm to make it readable to only those with special knowledge; this is referred to as a key. Using this cryptography concept, the conventional two-way relay channel can be interpreted from a new angle. In a two-way relay channel, during the MAC phase, user 1 and user 2 transmit message W_1 and W_2 to the relay, and the relay jointly detects and decodes the modulo sum of these two messages, i.e., $W_1 \oplus W_2$. This process can be thought as a type of encryption algorithm. During the BC phase, each user can decipher the encrypted message $W_1 \oplus W_2$ from the relay using its self-information as a key. Therefore, our encoding and decoding problem in the MIMO Gaussian K -way relay channel is to find the encryption algorithm so that all K users who take part in an information exchange can decode information from other users using their own self-information as a key.

The newly proposed encoding and decoding strategy involves a *signal space alignment for an encryption message* for the MAC phase and a *zero-forcing combined with successive network code decoding* for the BC phase. The key idea of the *signal space alignment for an encryption message* is that all users cooperatively design precoding vectors for transmitting a message so that the relay can receive a *proper encryption message*. Here, a proper encryption message is an encrypted message that all users who take part in the information exchange can resolve even if they all have different keys. In order for the relay to have the properly encrypted message, the each user selects the transmit signal direction for the encrypted information so that it has a special structure, *network code chain structure*. During the BC phase, *zero-forcing combined with successive network code decoding* enables all users to decipher the encryption message from the relay, even if they all have different self-information. Because the encryption message having a network code chain structure can be untangled successively at all users' side by using own side-information. From this decoding process, each user obtains the messages from the other users on the network.

The organization of this paper is followings: Section II describes the system model of the MIMO Gaussian K -way relay channel. In Section III, we compare the achievable degrees of freedom of the MIMO Gaussian K -way relay channel according to various schemes. Finally, Section IV concludes this paper.

Notation: We use bold upper and lower case letters for matrices and column vectors, respectively. $(\cdot)^T$ and $(\cdot)^H$

represent a transpose and a Hermitian transpose, respectively. $\mathbb{E}(\cdot)$ and $\text{Tr}(\mathbf{A})$ denote the expectation operator and trace of the matrix \mathbf{A} , respectively.

II. SYSTEM MODEL

The MIMO Gaussian K -way relay channel shown in Fig. 1 is considered in this section. In this channel, K users and a relay have M multiple antennas. The users want to exchange messages each other with the help of a single relay terminal. User i wants to send message W_i to the other users on the network and intends to decode all other users' messages on the network, i.e., $\{\hat{W}_1, \hat{W}_2, \dots, \hat{W}_K\} / \{\hat{W}_i\}$.

In multiple access (MAC) phase (the first time slot), user i sends message W_i to the relay. The received signal at the relay is represented by

$$\mathbf{y}^{[R]} = \sum_{i=1}^K \mathbf{H}^{[R,i]} \mathbf{x}^{[i]} + \mathbf{n}^{[R]}, \quad (1)$$

where $\mathbf{H}^{[R,i]}$ represents the $M \times M$ channel matrix from user i to the relay, $\mathbf{x}^{[i]} \in \mathbb{C}^M$ denotes transmit vector at user i , and $\mathbf{n}^{[R]} \in \mathbb{C}^M$ denotes an additive white Gaussian noise (AWGN) vector. The user has an average power constraint, $\mathbb{E}[\text{Tr}(\mathbf{x}^{[i]} \mathbf{x}^{[i]H})] \leq \text{SNR}$. The channel is assumed to be quasi-static and each entry of the channel matrix is an independently and identically distributed (i.i.d.) zero mean complex Gaussian random variable with unit variance, i.e., $\mathcal{NC}(0, 1)$.

After receiving, the relay generates new transmitting signals and broadcasts them to all users in what is known as, a BC phase. The received signal vector at user i is given by:

$$\mathbf{y}^{[i]} = \mathbf{H}^{[i,R]} \mathbf{x}^{[R]} + \mathbf{n}^{[i]}, \quad (2)$$

where $\mathbf{H}^{[i,R]}$ denotes the $M \times M$ channel matrix from the relay to user i , $\mathbf{x}^{[R]} \in \mathbb{C}^M$ is the transmit vector at the relay, and $\mathbf{n}^{[i]} \in \mathbb{C}^M$ denotes the AWGN vector. The transmit signal at the relay is subject to the average power constraint $\mathbb{E}[\text{Tr}(\mathbf{x}^{[R]} \mathbf{x}^{[R]H})] \leq \text{SNR}$. If the system is assumed to be in time-division-duplex (TDD) mode, the channel $\mathbf{H}^{[R,i]}$ is identical to $\mathbf{H}^{[i,R]H}$. However, it is assumed here that these two channels are generally different by taking into account frequency-division-duplex (FDD). Throughout this paper, direct links between users are neglected for simplicity; thus, the relay is essential for communication. Additionally, it is assumed that all users and the relay operate in half-duplex mode. This implies that all terminals can not receive and transmit simultaneously. The channel is assumed to be known perfectly at all users and the relay in both the transmit and receive modes.

A. Multicast capacity and degrees of freedom

By definition of multicast capacity in [17], we define the achievable rate for the multicast message W_i , as $R_i(\text{SNR})$, which is given by

$$R_i(\text{SNR}) = \min_{j=\{1,2,\dots,K\}/\{i\}} R_{ji}(\text{SNR}), \quad (3)$$

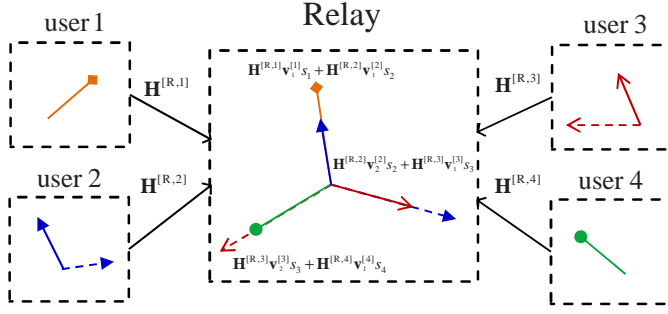


Fig. 2. Signal space alignment for encryption message for $K = 4$ case.

where $R_{ji}(\text{SNR})$ is the achievable rate from user i to user j , which is

$$R_{ji}(\text{SNR}) = \min \left\{ I(\mathbf{x}^{[i]}; \mathbf{y}^{[R]}), I(\mathbf{x}^{[R]}; \mathbf{y}^{[j]}) \right\}. \quad (4)$$

Therefore, the capacity region for the MIMO Gaussian K -way relay channel can be defined as the set of all achievable rate tuples $\mathbf{R}(\text{SNR}) = [R_1(\text{SNR}), R_2(\text{SNR}), \dots, R_K(\text{SNR})]^T$.

Furthermore, the degrees of freedom region for the MIMO Gaussian K -way relay channel is defined as in (5) (Please see the top of next page). In (5), $\mathbf{d} = (d_1, d_2, \dots, d_K)^T$, and $\mathbf{w} = (w_1, w_2, \dots, w_K)^T$. Accordingly, the sum of the degrees of freedom η is defined as

$$\eta \triangleq \max_{D^K \mathbf{w}} (d_1 + d_2 + \dots + d_K). \quad (6)$$

III. ACHIEVABLE DEGREES OF FREEDOM

In this section, we investigate the degrees of freedom that can be achieved according to various schemes for the MIMO Gaussian K -way relay channel. From this, we show that the proposed encoding and decoding scheme is able to attain the higher degrees of freedom in the MIMO Gaussian K -way relay channel by comparing with that achieved by a conventional time-division-multiple-access (TDMA) scheme.

A. TDMA scheme

In the MIMO Gaussian K -way relay channel, TDMA scheme requires $2K$ orthogonal time slots for completely exchanging the messages each other via a relay. In the first time slot, user 1 transmits the message W_1 using M independent streams to the relay. Thereafter, during the second time slot, the relay broadcasts the received message using M independent streams to all users (multicasting). By applying zero-forcing spatial decoder, each user can obtain the M independent streams and decodes them to get message, W_1 . In a similar way, user i , $\{i = 2, \dots, K\}$ can deliver the message to the other users via the relay by spending two orthogonal time slots. Therefore, the degrees of freedom that can be achieved TDMA scheme for the MIMO Gaussian K -way relay channel is given by:

$$\eta_{\text{TDMA}} = \frac{KM}{2K} = \frac{K-1}{2}, \quad \text{if } M = K-1. \quad (7)$$

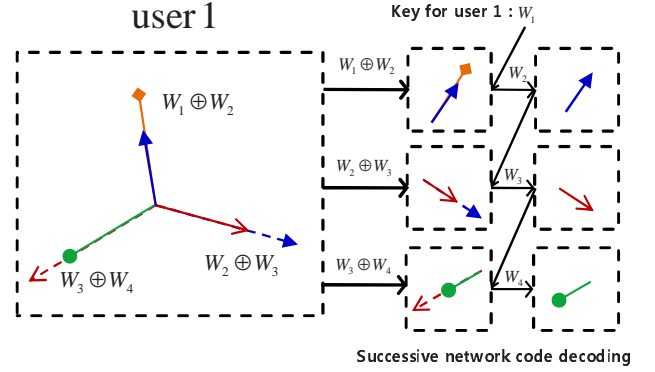


Fig. 3. Zero-forcing with successive network code decoding example of user 1 when $K = 4$.

B. Proposed scheme

The following theorem is the main result of this paper.

Theorem 1: In a MIMO Gaussian K -way relay channel where each user and the relay have $M = K - 1$ antennas, $\frac{K}{2}$ degrees of freedom is achievable for $K \geq 2$.

Proof: Here, we only show the case of $K = 4$ due to limitation of space. The journal version of this paper [19] includes the proof for the general K -user case and it shows that the proposed scheme can achieve the trivial outer bound derived by a cut-set theorem in [18]. The achievability proof is provided using signal space alignment for an encryption message and zero-forcing with successive network code decoding.

Using this encoding and decoding scheme, it is shown that $(d_1, d_2, d_3, d_4) = (1, 1, 1, 1)$, i.e., $\eta = \frac{\sum_{i=1}^K d_i}{2} = 2$ is achieved.

For the MAC phase (the first time slot), user 1 and user 4 send messages W_1 and W_4 using symbols s_1 and s_4 along with precoding vectors $\mathbf{v}_1^{[1]}$ and $\mathbf{v}_4^{[4]}$, as expressed by

$$\mathbf{x}^{[1]} = \mathbf{v}_1^{[1]} s_1, \quad \mathbf{x}^{[4]} = \mathbf{v}_4^{[4]} s_4, \quad (8)$$

while user 2 and user 3 transmit message W_2 and W_3 using symbol s_2 and s_3 . Here, we assume $\mathbb{E}[\|s_i\|^2] = 1$. Contrast with s_1 and s_4 , s_2 and s_3 are transmitted two times along with two different precoding vectors $\mathbf{v}_1^{[2]}$ and $\mathbf{v}_2^{[2]}$, as expressed by

$$\mathbf{x}^{[i]} = \mathbf{v}_1^{[i]} s_i + \mathbf{v}_2^{[i]} s_i, \quad i = \{2, 3\}. \quad (9)$$

The received signal at the relay is given by

$$\mathbf{y}^{[R]} = \sum_{i=1}^4 \mathbf{H}^{[R,i]} \left(\mathbf{v}_1^{[i]} s_i + \mathbf{v}_2^{[i]} s_i \right) + \mathbf{n}^{[R]}, \quad (10)$$

where $\mathbf{v}_2^{[1]} = \mathbf{v}_2^{[4]} = \mathbf{0}_{M \times 1}$.

The proposed precoding strategy is aiming at obtaining three network coding messages with chain property, $W^{[1]} \oplus W^{[2]}$, $W^{[2]} \oplus W^{[3]}$, $W^{[3]} \oplus W^{[4]}$ at the relay. Therefore, to accomplish this, precoding vectors are constructed by exploiting signal space alignment for network coding scheme [14]. Fig. 2 illustrates the conceptual figure of signal space alignment for an encryption message when $K = 4$. To decode $K-1 = 3$ network coded messages, $W^{[1]} \oplus W^{[2]}$, $W^{[2]} \oplus W^{[3]}$, $W^{[3]} \oplus W^{[4]}$

$$D^{Kw} \equiv \left\{ \mathbf{d} \in \mathbb{R}_+^K : \forall \mathbf{w} \in \mathbb{R}_+^K \quad \mathbf{w}^T \mathbf{d} \leq \lim_{\text{SNR} \rightarrow \infty} \left[\sup_{\mathcal{R}(\text{SNR}) \in C^{Kw}} \frac{\mathbf{w}^T \mathbf{R}(\text{SNR})}{\log(\text{SNR})} \right] \right\}. \quad (5)$$

at the relay, all users carefully chooses the precoding vectors in order to satisfy the conditions of signal space alignment for an encryption message. These are given by:

$$\begin{aligned} \text{span}(\mathbf{H}^{[R,1]} \mathbf{v}_1^{[1]}) &\doteq \text{span}(\mathbf{H}^{[R,2]} \mathbf{v}_1^{[2]}), \\ \text{span}(\mathbf{H}^{[R,2]} \mathbf{v}_2^{[2]}) &\doteq \text{span}(\mathbf{H}^{[R,3]} \mathbf{v}_1^{[3]}), \\ \text{span}(\mathbf{H}^{[R,3]} \mathbf{v}_2^{[3]}) &\doteq \text{span}(\mathbf{H}^{[R,4]} \mathbf{v}_1^{[4]}), \end{aligned} \quad (11)$$

where $\text{span}(\mathbf{A}) \doteq \text{span}(\mathbf{B})$ indicates that the column space of \mathbf{A} and \mathbf{B} are identical. The transmit beamforming vectors satisfying the conditions in (11) can be obtained by solving the *generalized eigenvalue problem* as

$$\begin{aligned} \mathbf{v}_1^{[1]} &= \alpha_1^{[1]} \mathbf{f}_1, & \mathbf{v}_1^{[2]} &= \alpha_1^{[2]} \mathbf{f}_1 \\ \mathbf{v}_2^{[2]} &= \alpha_2^{[2]} \mathbf{f}_2, & \mathbf{v}_1^{[3]} &= \alpha_1^{[3]} \mathbf{f}_2 \\ \mathbf{v}_2^{[3]} &= \alpha_2^{[3]} \mathbf{f}_3, & \mathbf{v}_1^{[4]} &= \alpha_1^{[4]} \mathbf{f}_3, \end{aligned} \quad (12)$$

where \mathbf{f}_1 , \mathbf{f}_2 , and \mathbf{f}_3 are eigenvectors that correspond to the maximum eigenvalues of matrices $(\mathbf{H}^{[R,1]} \mathbf{H}^{[R,2]})$, $(\mathbf{H}^{[R,2]} \mathbf{H}^{[R,3]})$, and $(\mathbf{H}^{[R,3]} \mathbf{H}^{[R,4]})$, respectively, and $\alpha_1^{[1]}$, $\alpha_1^{[2]}$, $\alpha_2^{[2]}$, $\alpha_1^{[3]}$, $\alpha_2^{[3]}$ and $\alpha_1^{[4]}$ are power normalization coefficients. These coefficients are determined to satisfy the following conditions as

$$\begin{aligned} \alpha_1^{[1]2} \|\mathbf{H}^{[R,1]} \mathbf{f}_1\|^2 &= \alpha_1^{[2]2} \|\mathbf{H}^{[R,2]} \mathbf{f}_1\|^2, \\ \alpha_2^{[2]2} \|\mathbf{H}^{[R,2]} \mathbf{f}_2\|^2 &= \alpha_1^{[3]2} \|\mathbf{H}^{[R,3]} \mathbf{f}_2\|^2, \\ \alpha_2^{[3]2} \|\mathbf{H}^{[R,3]} \mathbf{f}_3\|^2 &= \alpha_1^{[4]2} \|\mathbf{H}^{[R,4]} \mathbf{f}_3\|^2, \\ \alpha_1^{[i]2} + \alpha_2^{[i]2} &\leq \text{SNR}, \quad \forall i, \end{aligned} \quad (13)$$

where $\alpha_2^{[1]} = \alpha_2^{[4]} = 0$. For example, if $\|\mathbf{H}^{[R,1]} \mathbf{f}_1\|^2 < \|\mathbf{H}^{[R,2]} \mathbf{f}_1\|^2$, we design $\alpha_1^{[1]2} = \text{SNR}/2$. By doing so, $\alpha_1^{[2]2} < \text{SNR}/2$. In addition, if $\|\mathbf{H}^{[R,2]} \mathbf{f}_2\|^2 < \|\mathbf{H}^{[R,3]} \mathbf{f}_3\|^2$, we also design $\alpha_2^{[2]2} = \text{SNR}/2$. Therefore, user 2 can satisfy the transmit power constraint, $\alpha_1^{[2]2} + \alpha_2^{[2]2} \leq \text{SNR}$. In a similar way, all power normalizing coefficients can be calculated so that the output magnitude of two vectors on the same signal dimension of the relay are the same while satisfying the transmit power constraint of all users.

As the result, the received signal at the relay in (10) becomes

$$\begin{aligned} \mathbf{y}^{[R]} &= \begin{bmatrix} \mathbf{u}_1 & \mathbf{u}_2 & \mathbf{u}_3 \end{bmatrix} \begin{bmatrix} s_1 + s_2 \\ s_2 + s_3 \\ s_3 + s_4 \end{bmatrix} + \mathbf{n}^{[R]}, \quad (14) \\ &= \mathbf{U}^{[R]} \mathbf{s}^{[R]} + \mathbf{n}^{[R]}, \end{aligned}$$

where $\mathbf{u}_1 = \mathbf{H}^{[R,1]} \mathbf{v}_1^{[1]} = \mathbf{H}^{[R,2]} \mathbf{v}_1^{[2]}$, $\mathbf{u}_2 = \mathbf{H}^{[R,2]} \mathbf{v}_2^{[2]} = \mathbf{H}^{[R,3]} \mathbf{v}_1^{[3]}$, and $\mathbf{u}_3 = \mathbf{H}^{[R,3]} \mathbf{v}_2^{[3]} = \mathbf{H}^{[R,4]} \mathbf{v}_1^{[4]}$. In (14), $\mathbf{U}^{[R]}$ denotes the effective channel matrix. At this point, it

is necessary to check the decodability of $\mathbf{s}^{[R]}$ at the receiver of the relay. The decodability is simply proved by showing that $\Pr[\det(\mathbf{U}^{[R]}) = 0] = 0$. Recall that \mathbf{u}_i , $i = \{1, 2, 3\}$, is one of the M intersection basis vectors between $\mathbf{H}^{[R,i]}$ and $\mathbf{H}^{[R,i+1]}$. In addition, we define a subspace, V_i^c , consisted by basis vectors $\{\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3\} - \{\mathbf{u}_i\}$. As the entries of $\mathbf{H}^{[R,i]}$ are generated by a continuous distribution, the probability that a basis vector in the intersection of any two channel matrices lies in the other intersection subspace spanned by the other two channel matrices is zero, i.e., $\Pr[\mathbf{u}_i \subset V_i^c] = 0$, $\forall i$. Consequently, this gives

$$\Pr[\det(\mathbf{U}^{[R]}) = 0] \leq \sum_{i=1}^3 \Pr[\mathbf{u}_i \subset V_i^c] = 0. \quad (15)$$

Therefore, $\mathbf{s}^{[R]}$ can be obtained by eliminating the inter-signal space interference using a zero-forcing decoder, which is

$$\mathbf{s}^{[R]} = \mathbf{U}^{[R]-1} \mathbf{y}^{[R]} + \mathbf{U}^{[R]-1} \mathbf{n}^{[R]}. \quad (16)$$

The three network coded messages $\hat{W}_{\pi(1,2)}^{[R]} = W_1 \oplus W_2$, $\hat{W}_{\pi(2,3)}^{[R]} = W_2 \oplus W_3$, and $\hat{W}_{\pi(3,4)}^{[R]} = W_3 \oplus W_4$ are then obtained by applying the physical-layer network coding (PNC) modulation-demodulation mapping principle [8] into each symbol $s_i^{[R]}$ via a signal dimension.

During the BC phase (the second time slot), the relay broadcasts three encrypted information $\hat{W}_{\pi(1,2)}^{[R]} = W_1 \oplus W_2$, $\hat{W}_{\pi(2,3)}^{[R]} = W_2 \oplus W_3$, and $\hat{W}_{\pi(3,4)}^{[R]} = W_3 \oplus W_4$ to all users using 3 encoded symbols $[q_1^{[R]}, q_2^{[R]}, q_3^{[R]}]$ along beamforming vectors $[\mathbf{v}_1^{[R]}, \mathbf{v}_2^{[R]}, \mathbf{v}_3^{[R]}]$. This is denoted as follows:

$$\mathbf{x}^{[R]} = \sum_{i=1}^3 \mathbf{v}_i^{[R]} q_i^{[R]}, \quad i = 1, 2, 3. \quad (17)$$

The received signal at user i can be expressed as

$$\begin{aligned} \mathbf{y}^{[i]} &= \mathbf{H}^{[i,R]} \mathbf{x}^{[R]} + \mathbf{n}^{[i]}, \\ &= \mathbf{H}^{[i,R]} \sum_{i=1}^3 \mathbf{v}_i^{[R]} q_i^{[R]} + \mathbf{n}^{[i]}, \\ &= \mathbf{Q}^{[i,R]} \mathbf{q}^{[R]} + \mathbf{n}^{[i]}, \end{aligned} \quad (18)$$

where $\mathbf{Q}^{[i,R]}$ denotes the effective channel from the relay to user i , and $\mathbf{q}^{[R]} = [q_1^{[R]}, q_2^{[R]}, q_3^{[R]}]^T$. In this case, to detect the symbol $\mathbf{q}^{[R]}$ at user i , the effective channel, $\mathbf{Q}^{[i,R]}$ should be invertible. This condition is guaranteed if the precoding matrix $\mathbf{V}^{[R]} = [\mathbf{v}_1^{[R]}, \mathbf{v}_2^{[R]}, \mathbf{v}_3^{[R]}]$ has the rank of 3 due to the fact that the rank of the product of two square matrices \mathbf{A} and \mathbf{B} cannot exceed the smallest rank of the multiplicand matrices. In other words, all effective channels $\mathbf{Q}^{[i,R]}$, $i = \{1, 2, 3\}$

TABLE I
THE SUM OF ACHIEVABLE DEGREES OF FREEDOM WHEN $K = 4$.

Scheme	Sum of degrees of freedom (η)	Number of antennas (M)
TDMA	$\frac{K-1}{2} = \frac{3}{2}$	$K - 1 = 3$
Proposed	$\frac{K}{2} = 2$	$K - 1 = 3$

have full rank if $\mathbf{V}^{[R]}$ has the 3 rank, as all downlink channels from the relay to the users almost likely have the rank of 3. Therefore, the conclusion is that all users are able to detect $\mathbf{q}^{[R]}$ by zero-forcing detection, which nulls out the inter-signal space interference. For user i , the detected signal is

$$\mathbf{q}^{[R]} = \mathbf{Q}^{[i,R]^{-1}} \mathbf{y}^{[i]} + \mathbf{Q}^{[i,R]^{-1}} \mathbf{n}^{[i]}. \quad (19)$$

After detection $\mathbf{q}^{[R]}$, each user decodes the messages from the other users by resolving the encrypted message, $W_{\pi(i,i+1)}^{[R]} = W_i \oplus W_{i+1}$, $i = \{1, 2, 3\}$, which is contained in $\mathbf{q}^{[R]}$. The decryption procedure is performed by successive network code decoding scheme shown in Fig. 3. Considering the receiver of user 1, here, user 1 wants to decode \hat{W}_2, \hat{W}_3 , and \hat{W}_4 , reliable which are the messages coming from user 2, user 3, and user 4, respectively. By exploiting self-information W_1 as a key, user 1 first extracts \hat{W}_2 from message $W_1^{[R]} = W_1 \oplus W_2$ contained in $q_1^{[R]}$, as follows:

$$\hat{W}_2 = W_1^{[R]} \oplus W_1 = (W_1 \oplus W_2) \oplus W_1. \quad (20)$$

Subsequently, user 1 successively decodes \hat{W}_3 from message $W_2^{[R]} = (W_2 \oplus W_3)$, which is contained in $q_2^{[R]}$ using message W_2 as another key; this is decoded message from the previous step. In this consecutive approach, user 1 untangles the network code chain successively. Eventually, user 1 is able to obtain all messages \hat{W}_2, \hat{W}_3 , and \hat{W}_4 from the other users.

In the same manner, other all users can resolve the encrypted message $W_{\pi(i,i+1)}^{[R]} = W_i \oplus W_{i+1}$, $i = \{1, 2, 3\}$. Therefore, $\frac{K}{2} = \frac{4}{2} = 2$ degrees of freedom can be achieved on the MIMO Gaussian 4-way relay channel. In other word, *4 users can exchange information each other within two time slots on the MIMO Gaussian 4-way relay channel if all nodes have $M = K - 1 = 3$ antennas.*

Therefore, the achievable degrees of freedom of the MIMO Gaussian 4-way relay channel according to two schemes is summarized as shown in TABLE I.

Remark 1: In the Gaussian single-input-single-output (SISO) K -way relay channel, $\frac{K}{K-1}$ degrees of freedom can be achieved if the channel coefficients are time/frequency variant. In this case, the precoding vectors for the signal space alignment for an encryption message are designed over the $K - 1$ time/frequency slots, similar to the method used in [16].

Remark 2: In the BC phase, the relay transmits the encrypted messages with the network code chain structure. Assuming that an eavesdropper having M antennas wants to decode the messages during the BC phase, the question arises as to how many messages the eavesdropper can reliably decode. The proposed coding strategy only allows the users who participate

in the message exchange via relay to decipher the messages, as the users who take part have the key to crack the network code chain. Therefore, due to the absence of knowledge regarding a certain key, the eavesdropper cannot decode any message. It indicates that the proposed scheme is robust in terms of the message security.

IV. CONCLUSIONS

In the MIMO Gaussian K -way relay channel, we proposed an encoding and decoding strategies inspired from cryptography. It involves *signal space alignment for an encryption message and zero forcing combined with successive network code decoding*. Using this encoding decoding scheme, it was shown that the proposed scheme can achieve the higher degrees of freedom as compared with that of TDMA scheme.

REFERENCES

- [1] C. E. Shannon, "Two-way communication channels," *In Proc. 4th Berkeley Symp. Math. Stat. Prob.*, vol. 1, pp. 611-644, Berkeley, CA, 1961.
- [2] B. Rankov and A. Wittneben, "Spectral efficient protocols for half-duplex fading relay channels," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 2, pp. 379-389, Feb. 2007.
- [3] B. Rankov and A. Wittneben, "Achievable rate regions for the two-way relay channel," *IEEE International Symposium on Information Theory, ISIT*, Seattle, USA, July 9-14, 2006.
- [4] N. Lee, H. Park, and J. Chun, "Linear precoder and decoder design for two-way AF MIMO relaying system," *IEEE VTC 2008 Spring*, pp. 1221-1225, May 2008.
- [5] K. Narayanan, M. P. Wilson, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," *in Proc. 45th Allerton Conf. on Commun., Control, and Comput.*, Monticello, IL, Sep., 2007.
- [6] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," *Computer Science and Artificial Intelligence Laboratory Technical Report*, MIT-CSAIL-TR-2007-012, Feb. 2007.
- [7] S. Katti, H. Rahul, W. Hu, D. Katabi, M. Medard, and J. Crowcroft, "XORs in the Air: Practical Wireless Network Coding," *ACM SIGCOMM*, Pisa, Italy, Sep. 11-15, 2006.
- [8] S. Zhang, S. -C. Liew, and P. P. Lam, "Physical layer network coding," *arXiv:0704.2475v1*.
- [9] S. Zhang, S. -C. Liew, and L. Lu, "Physical layer network coding schemes over finite and infinite fields," *arXiv:0804.2058v1*.
- [10] M. Chen and A. Yener, "Multiuser two-way relaying for interference-limited systems," *IEEE International Conference on Communication, ICC 2008 May 2008*.
- [11] S. Avestimehr, M. A. Khajehnejad, A. Sezgin, and B. Hassibi, "Capacity region of the deterministic multi-pair bi-directional relay network," *in Proc. of IEEE ITW 2009, Volos, Greece*, June, 2009.
- [12] A. Sezgin, M. A. Khajehnejad, S. Avestimehr, and B. Hassibi, "Approximate capacity region of the two-pair bidirectional Gaussian relay network," *in Proc. of ISIT 2009, Seoul, Korea*, June, 2009.
- [13] D. Gunduz, A. Yener, A. Goldsmith, and H. V. Poor, "The multi-way relay channel," *in Proc. of ISIT 2009, Seoul, Korea*, June, 2009.
- [14] N. Lee and J. -B. Lee, "A novel signaling on the MIMO Y channel: signal space alignment for network coding," *IEEE ISIT 2009, Seoul*, July 2009.
- [15] N. Lee, J. -B. Lee, and J. Chun, "Degrees of freedom on the MIMO Y channel: signal space alignment for network coding," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, July 2010.
- [16] V. R. Cadambe and S. Jafar, "Interference alignment and degrees of freedom of the K -User interference channel," *IEEE Trans. Inf. Theory*, vol. 54, pp. 3425-3441, Aug. 2008.
- [17] N. Jindal and Z.-Q. Luo, "Capacity limits of multiple antenna multicast," *in Proc. IEEE Int. Symp. Inf. Theory*, July, 2006.
- [18] T. M. Cover and J. A. Thomas, "Elements of Information Theory." New York: Wiley-Interscience, 1991.
- [19] N. Lee, and J. Chun, "Degrees of Freedom on a MIMO Gaussian K -way Relay Channel: An Encryption and Decryption Approach," *Submitted to IEEE Trans. Inf. Theory*, April 2010.